

Applicant: Pinkas et al.
Application No.: 09/807,099
Examiner: L. Son

Remarks

Claims 1-22 are presented for the Examiner's review and consideration. Claim 1-3 and 17 have been amended. Applicants believe the claim amendments and the accompanying remarks herein serve to clarify the present invention and are independent of patentability. No new matter has been added.

35 U.S.C. §102 Rejection based on Shoham

Claims 1-3, 5-8, 10-11, and 16 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,285,989 to Shoham ("Shoham"). For the reasons set forth below, Applicants respectfully submit that this rejection should be withdrawn.

Shoham discloses a method and apparatus for designing and deploying a universal, interactive, real-time, on-line trading market system serving traders communicating via the Internet and similar networks. (Col. 5, lns. 6-9). Referring to FIG. 1, the present invention includes the following primary components: (Col. 5, lns. 18-19).

3. A Universal Trading Console (UTC) 120. This component consists of a computer running a program, which enables a trader to trade in any market protocol executing on the PAS 140. The UTC 120 presents to the trader information in a way that automatically adapts to the specific market protocol executing, and allows the trader to participate in the trading. (Col 5, lns 36-42).

4. A Universal Surveillance Console (USC) 130. This component consists of a computer running a program which enables a surveillance body--such as a regulatory agency or and independent audit firm--to monitor the operation of the markets executing on the PAS 140, ascertain that the execution conforms to norms, and optionally intervene in the market when deviations are detected. (Col 5, lns 43-49).

The UTC 120 offers the trader two functionalities--display of information, and bid input. (Col. 10, lns. 26-27). The information displayed to the user is of kinds: 1) activities on the PAS 140, and 2) ancillary information. (Col. 10, lns. 27-29). Ancillary information may be any information that is relevant to making trade decisions but that is not inherent in the market activity. Col. 10, lns. 41-43).

The USC 130 is much like the UTC 120, in that it presents to the surveillance agency information from the marketplace. (Col. 11, lns. 12-14). Every professional trading market is

Applicant: Pinkas et al.
Application No.: 09/807,099
Examiner: L. Son

associate with one or more surveillance bodies, whose job it is to monitor the trading activities and ensure that they adhere to certain standards. (Col. 11, Ins. 2-5). The primary difference is that the USC 130 does not provide for ways in which to trade in the market, but on the other hand does provide market controls that are not provided to traders. (Col. 11, Ins. 14-17).

As such, Shoham discloses an interactive, real-time, on-line trading market system which includes at least two consoles. A UTC console for providing a trader with trading information and allowing a trader to make trades on the system. A USC console for use by a surveillance agency, allowing the surveillance agency to monitor the trading activities and ensure that they adhere to certain standards. However, Shoham fails to disclose that the USC console provides information to the individual traders for monitoring the trading active, i.e., calculating a function F and providing additional information, a proof, to each user to verify the trades were computed correctly.

In contrast, the present invention relates generally to cryptography and to secure distributed computation, and more particularly it relates to computerized auctions conducted using PCs and/or servers over a network, such as, the Internet. (Page 1, Ins. 8-10). Consider a scenario with N parties, each having a private input, and a single center. (Page 3, Ins. 21-22). There is a function F with N inputs whose output should be computed. (Page 3, ln. 22). The present invention is a method, system and apparatus that enables the center to compute and publish the output of F and to prove to all parties that it computed F correctly. (Page 3, Ins. 23-25). This is done without revealing the value of the input of a party to any other party. (Page 3, Ins. 25-26).

The center announces Step 301 that it will compute the function F . (In the case of an auction the auctioneer announces the existence of the auction and publishes its rules). (Page 8, Ins. 6-8). The center now computes in Step 308 the value of the circuit that computes F for the inputs $x_{sub.i}$ it received. (Page 8, Ins. 27-28). The center computes and publishes a proof in Step 309 that it computed the value of F correctly. (Page 8, Ins. 29-30). Each party can use the published commitments to verify in Step 310 that the proof is correct. (Page 8, Ins. 30-31).

As such, the present invention discloses an auction system which computes an output for a function F . The function F which is computed is based on the input of the users. The system

Applicant: Pinkas et al.
Application No.: 09/807,099
Examiner: L. Son

provides the output for the function F to the users, as well as a proof of the correctness of the output calculation. Shoham fails to disclose calculating and providing an output for a function F to each user and providing a proof of correctness of the output to the each user, but instead, discloses a USC terminal for use by a surveillance company to verify the correctness of the trades.

Independent claim 1 recites, *in part*, the step of publishing by center A additional to each of the users information which lets each of the users verify that F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, $F(X_{\text{sub.1}}, \dots, X_{\text{sub.n}})$, and from their own inputs, and (ii) information about the inputs of other users.

In light of the foregoing, independent claim 1 is respectfully submitted to be patentable over Shoham. As claims 2, 3, 5-8, 10-11, and 16 depend from claim 1 these dependent claims necessarily include all the elements of their base claim. Accordingly, Applicants respectfully submit that the dependent claims are allowable over Shoham at least for the same reasons.

35 U.S.C. §103 Rejections

Claim 9 was rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham as applied to claim 1. Claims 4, 8, and 12-14 were rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham in view of U.S. Patent No. 6,021,398 to Ausubel. Claim 15 was rejected under 35 U.S.C. 103(a) as being unpatentable over Shoham in view of U.S. Patent No. 6,055,508 to Naor et al. ("Naor").

Claims 4, 8, 9, and 12-15 depend from claim 1. As noted above claim 1 is patentable over Shoham. The inclusion of Ausubel or Naor fails to overcome the deficiencies in Shoham. Accordingly, Applicants respectfully submit that the dependent claims are allowable over Shoham at least for the same reasons.

Claims 17-22 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,055,518 to Franklin et al. ("Franklin") in view of Naor. For the reasons set forth below, Applicants respectfully submit that this rejection should be withdrawn.

The Examiner states that Franklin does not teach a second program provided to the

Applicant: Pinkas et al.
Application No.: 09/807,099
Examiner: L. Son

parties enabling each of said parties to prove that said function F was calculated correctly. Nevertheless, the Examiner states that Naor does teach a method of providing an auditing program to certify multiple transactions between the plurality clients and serves and able to correlate against the server calculation to proof the result.

Franklin discloses a secure auction service for use in a network having servers and bidding terminals. (Abstract). The secure auction system of the present invention provides an interface or bidding terminals by which clients or bidders can issue secret bids to the auction servers for an advertised auction. (Col. 2, lns. 22-25). Once the bidding period is closed, the auction service opens the bids, determines the winning bid, and provides the winning bidder with a ticket for claiming the item bid upon. (Col. 2, lns. 25-28). Using novel cryptographic techniques, the secure auction system is constructed to provide strong protection for both the auction house and correct bidders, despite the malicious behavior of any number of bidders and fewer than one-third of the servers comprising the secured auction system. (Col. 2, lns. 28-33).

Naor discloses a method for accounting and auditing of communications networks. (Col. 1, lns. 6-7). The present invention relates to methods for measuring the amount of service requested from servers by clients in a communications network. The methods are secure and efficient, and provide a short proof for the metered data. (Col. 6, lns. 24-26). The principal property of the metering method of the present invention is that the server is able to present to an auditor a short proof for the number of services it has performed. (Col. 7, lns 12-15). An auditor can verify this proof. (Col. 7, ln. 15).

Initially, Applicants note that Franklin discloses a secure auction server and Naor discloses a method of measuring the amount of services requested from servers by clients. As such, Franklin and Naor are directed to non-related subject matter and there is no motivation to combine the two references.

Furthermore, Naor discloses that the method of measuring the amount of service requested by the clients includes providing the metered data only to an auditor, where a short proof of the metered data is additionally provided to the auditor. Naor fails to disclose that the metered data or the proof is provided to the individual clients.

In contrast claim 17 recites, *inter alia*, a system that contains N parties, each having a

Applicant: Pinkas et al.
Application No.: 09/807,099
Examiner: L. Son

private input, and a center adapted to compute a function F of the input. An apparatus for computing the function F in the center includes a first program provided in the center that enables calculation of the function F . Circuitry for publishing the function F , to each of the N parties, using the program while not revealing substantially any information about the input; and a second program provided to the parties enabling each one of said parties to prove that the function F was calculated correctly.

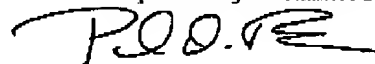
In light of the foregoing, independent claim 17 is respectfully submitted to be patentable over Franklin in view of Naor. As claims 18-22 depend from claim 17 these dependent claims necessarily include all the elements of their base claim. Accordingly, Applicants respectfully submit that the dependent claims are allowable over Franklin in view of Naor at least for the same reasons.

Conclusion

In light of the foregoing remarks, this application is now in condition for allowance and early passage of this case to issue is respectfully requested. If any questions remain regarding this amendment or the application in general, a telephone call to the undersigned would be appreciated since this should expedite the prosecution of the application for all concerned.

No fee is believed to be due. However, please charge any required fee (or credit any overpayments of fees) to the Deposit Account of the undersigned, Account No. 500601 (Docket No. 704-X00-047US).

Respectfully submitted,


PAUL D. BIANCO Reg # 43,500
For Martin Fleit, Reg. # 16,900

Customer Number: 27317

Martin Fleit

FLEIT KAIN GIBBONS GUTMAN BONGINI & BIANCO, P.L.

601 Brickell Key Drive, Suite 404

Miami, Florida 33131

Tel: 305-416-4490; Fax: 305-416-4489

e-mail: mfleit@focusnip.com